Cybersecurity Mini Risk Assessment

1. *Create a prioritized risk assessment:

A risk assessment should be the first step toward identifying and prioritizing what areas of cybersecurity are a concern and need addressing.

☐ Done ☐ In Progress ☐ Not Started

Notes:

2. *Implement Multi-factor Authentication (MFA):

MFA is a cornerstone for security and should be used on all critical and public-facing systems (i.e., servers, email, workstations, cloud systems).

☐ Done ☐ In Progress ☐ Not Started

Notes:

3. *Conduct Security Awareness Training:

The greatest risk within an organization is its end-users. Most security incidents are caused by human error. Train employees in cybersecurity best practices on a regular basis.

☐ Done ☐ In Progress ☐ Not Started

Notes:

4. *Manage Hardware and Software Lifecycle:

As products age, they often become obsolete (i.e., Windows 7, Windows 10 in 4th quarter 2025) and no longer supported. Knowing the lifecycle allows for replacement (i.e., switches, firewalls, PCs) or upgrades ahead of potential threats.

☐ Done ☐ In Progress ☐ Not Started

Notes:

5. *Endpoint Detection (Standardized):

Ensure your devices and data are protected from malware and cyberattack with advanced endpoint detection and response tools that are standardized and kept up-to-date.

☐ Done ☐ In Progress ☐ Not Started

Notes:

6. *Complete Vulnerability Assessments:

Regular scans of the internal and external networks help identify where vulnerabilities exist so that they may be mitigated.

☐ Done ☐ In Progress ☐ Not Started

Notes:

7. *Patch Management Program

Fixing vulnerabilities and keeping systems current help manage and reduce the risk that exists in an environment. It is especially important in minimizing a ransomware attack.

☐ Done ☐ In Progress ☐ Not Started

Notes:

8. *Maintain Full Backups:

Backups of your data could be the difference between a complete loss or a complete recovery in the event of an attack (i.e., ransomware) or a disaster. Backup servers and use backup locally (i.e., OneDrive). Verify backups.

☐ Done ☐ In Progress ☐ Not Started

Notes:

Cybersecurity Mini Risk Assessment

9. *Least Privilege:

Remove administrator privileges from all accounts and limit who has administrative use. Elevate administrative tasks only when necessary. Only provide the necessary security for users to do their jobs, nothing more.

☐ Done ☐ In Progress ☐ Not Started

Notes:

10. *Perimeter Review:

The firewall is typically the first defense barrier. Improperly configured devices are useless. Review configurations for completeness, remove obsolete entries, and, above all, make sure there is one. Explore Intrusion Detection Systems and the use of DMZs.

☐ Done ☐ In Progress ☐ Not Started

Notes:

11. *Email, DNS, DLP, and Web Filtering:

The origin of most cyberattacks are from email and websites. Filters help secure organizations by eliminating known and possible threats. Implement Data Loss Prevention (DLP) filters to ensure PII is sent securely.

☐ Done ☐ In Progress ☐ Not Started

Notes:

12. *TLD Migration:

Anyone can register a .com, .org, or .us domain. This is hard for anyone to know who an organization claims to be. The .gov and .edu domains are different and only available to US-based government and educational organizations. The public should not have to guess whether a website or an email is genuine.

☐ Done ☐ In Progress ☐ Not Started

Notes:

13. Develop an Incident Response Plan:

Allows organizations to identify, protect, detect, respond, and recover from security breaches. This proactive approach ensures that the incident is isolated, helping to prevent spread or further damage.

☐ Done ☐ In Progress ☐ Not Started

Notes:

14. Cybersecurity Insurance:

Governments are the third-most targeted industry. Cyber insurance provides important coverage to those suffering from an attack.

☐ Done ☐ In Progress ☐ Not Started

Notes:

15. Encryption:

Ensures effective security where information cannot be intercepted and used. At rest protects data from unauthorized access in theft, loss, or physical damage. In transit protects data from interception, eavesdropping, and tampering during transmission.

☐ Done ☐ In Progress ☐ Not Started

Notes:

16. Mobile Device Management:

MDM helps organizations ensure that information on devices do not fall into the hands of cyber criminals and minimizes the risk of devices being infected by malware or other viruses that hackers use to compromise or steal sensitive data.

☐ Done ☐ In Progress ☐ Not Started

Notes:

Cybersecurity Mini Risk Assessment

17. CISA Services:

CISA has several excellent services that are required for grant funding but are free, including an external vulnerability scan and a risk assessment.

☐ Done ☐ In Progress ☐ Not Started

Notes:

18. ISAC (MS-ISAC/WaterISAC):

Benefits include access to cybersecurity advisories and alerts, vulnerability assessments and incident response, secure information sharing, tabletop exercises, malicious domain report, training resources, and incident mitigation.

☐ Done ☐ In Progress ☐ Not Started

Notes:

19. Plan Testing:

An important, coordinated exercise to scenarios that could happen to your organization. Key personnel gather to walk through disastrous scenarios and see if plans actually make sense in response to various disasters, natural or manmade.

☐ Done ☐ In Progress ☐ Not Started

Notes:

20. Rogue Device Detection:

Not knowing all the devices connected to your network could result in a major attack. Using detection tools to alert when an unknown or unauthorize device connects will help minimize disruptions.

☐ Done ☐ In Progress ☐ Not Started

Notes:

21. Change Default Passwords:

Default passwords should always be removed from devices and systems to prevent introducing a simple means of being susceptible to attack.

☐ Done ☐ In Progress ☐ Not Started

Notes:

22. Enhanced logging and alerting:

Log collection, analysis and alerting will be invaluable following an attack. Central management will allow for filtering of the most significant data.

☐ Done ☐ In Progress ☐ Not Started

Notes:

23. Disable Macros

Macros are often part of phishing campaigns that send infected scripts that enable unauthorized access or include a macro virus. Most users never use macros.

☐ Done ☐ In Progress ☐ Not Started

Notes:

24. Asset Management

To effectively manage risk, you must first know what is at risk; including servers, PCs, network infrastructure, IOT devices, software. Create network topologies.

☐ Done ☐ In Progress ☐ Not Started

Notes:

25. Governance

Is there support from organization management/stakeholders? Are there adequate resources? Is the budget sufficient?

☐ Done ☐ In Progress ☐ Not Started

Notes:

Cybersecurity Mini Risk Assessment

- Attach supporting documentation for at least those risks preceded by an asterisk. For example, show your endpoint detection solution including number of users.
- If you marked "NOT STARTED", what's your plan to mitigate the risk and have it completed? Indicate separately, using a separate sheet, if necessary, the plan for each risk marked Not Started.
    - If unsure how to answer, seek guidance from your IT professional, in-house or outsourced.
- The numbers shown for each risk are for identification purposes only. These are not to be considered as listed in order of priority. The priority may be different for each organization.
- Those items marked with an asterisk are top priorities.
- This assessment must be completed with the entire organization (municipality, county, education, etc.) as a whole in mind and not a specific area or department (i.e., water or sewage).